Recovery Act
Subtitle D - Privacy Review
Summary

Title / Section	Link to Detail
Subtitle D -- Privacy	
Sec. 13400 Definitions	
PLEASE NOTE: This column may not include full definitions and only an outline or summary of the highlighted section. Please use the link to obtain full ARRA 09 language.	
BREACH - The term "breach" means the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.	Detail Information
ELECTRONIC HEALTH RECORD - The term ‘‘electronic health record’’ means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.	Detail Information
PERSONAL HEALTH RECORD - The term "personal health record" means an electronic record of PHR identifiable health information (as defined in section 13407 (f)(2) on an individual that can be drawn from multiple sources and that is· managed, shared, and controlled by or primarily for the individual.	Detail Information
STATE - The term ‘‘State’’ means each of the several States, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Northern Mariana Islands.	Detail Information

Recovery Act
Subtitle D - Privacy Review

Title / Section	Link to Detail
Subtitle D -- Privacy	
VENDOR OF PERSONAL HEALTH RECORDS - The term ‘‘vendor of personal health records’’ means an entity, other than a covered entity (as defined in paragraph (3)), that offers or maintains a personal health record.	Detail Information
PART I -- IMPROVED PRIVACY PROVISIONS AND SECURITY PROVISIONS	
Sec. 13041 APPLICATION OF PRIVACY PROVISIONS AND PENALTIES TO BUSINESS ASSOCIASTE OF COVERED ENTITIES; ANNUAL GUIDANCE ON SECURITY PROVISIONS	
Entities that are known as a business associate of a covered entity (as defined in the HIPAA Privacy rule) shall also be required to follow all Security requirements in the same manner that such sections apply to the covered entity. The business associate agreements that have been executed between covered entity and the third party vendor will need to incorporate specific language to this affect.	Detail Information
CIVIL AND CRIMINAL PENALTIES will now be applied to a business associate that violates any security provision specified in subsection (a), sections 1176 and 1177 of the Social Security Act (42 U.S.C. 1320d–5, 1320d–6) in the same manner such sections apply to a covered entity that violates such security provision.	Detail Information

Recovery Act
Subtitle D - Privacy Review

Title / Section	Link to Detail
Subtitle D -- Privacy	
Sec. 13402 NOTIFICATION IN THE CASE OF BREACH	
Specific notification requirements when a breach of data has been established for information that has not been encrypted or made non-readible. The language requires notification to an individual if their information is subject to an unauthorized use or disclosure.	Detail Information
A business associate of a covered entity, upon discovery of a breach, shall notify the covered entity of such breach.	Detail Information
A breach shall be treated as discovered by a covered entity or by a business associate as of the first day on which such breach is known to such entity or associate.	Detail Information
Notice of a breach must be provided within 60 calendar days after discovery. Covered Entities and Business Associates will be required to show they have acted in an appropriate manner.	Detail Information
Specific methods of notification to an individual are provided in the regulations.	Detail Information

Recovery Act
Subtitle D - Privacy Review

Title / Section	Link to Detail
Subtitle D -- Privacy	
HHS will begin posting on the HHS public web site all incidents in which the unsecured protected health information of more than 500 individuals is acquired or disclosed.	Detail Information
Specific contents of the notice are outlined in the regulations.	Detail Information
UNSECURED PROTECTED HEALTH INFORMATION - protected health information that is not secured through the use of a technology or methodology specified by the Secretary in the guidance issued under paragraph (2).	Detail Information
Not later than 60 days after the date of the enactment of this Act, the Secretary shall issue guidance specifying the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals.	Detail Information
REGULATIONS; EFFECTIVE DATE - The Secretary of Health and Human Services shall promulgate interim final regulations within 180 days after the date of the enactment of this title. The provisions of this section shall apply to breaches that are discovered on or after the date that is 30 days after the date of publication of such interim final regulations.	Detail Information

Recovery Act
Subtitle D - Privacy Review

Title / Section	Link to Detail
Subtitle D -- Privacy	
Sec. 13403 EDUCATION ON HEALTH INFORMATION PRIVACY	
REGIONAL OFFICE PRIVACY ADVISORS - Within 6 months after the date of the enactment of this Act, the Secretary shall designate an individual in each regional office of the Department of Health and Human Services to offer guidance and education. EDUCATION INITIATIVE ON USES OF HEALTH INFORMATION - Within 12 months after the date of the enactment of this Act, the Office for Civil Rights shall develop and maintain a multi-faceted national education initiative to enhance public transparency regarding the uses of protected health information.	Detail Information
Sec. 13404 APPLICATION OF PRIVACY PROVISIONS AND PENALTIES TO BUSINESS ASSOCIATES OF COVERED ENTITIES	
APPLICATION OF CONTRACT REQUIREMENTS.—In the case of a business associate of a covered entity that obtains or creates protected health information, the business associate may use and disclose such protected health information. The additional requirements of this subtitle that relate to privacy and that are made applicable with respect to covered entities shall also be applicable to such a business associate and shall be incorporated into the business associate agreement between the business associate and the covered entity.	Detail Information

Recovery Act
Subtitle D - Privacy Review

Title / Section	Link to Detail
Subtitle D -- Privacy	
APPLICATION OF CIVIL AND CRIMINAL PENALTIES - Penalties are now extending to business associates and their associates.	Detail Information
Sec. 13405 RESTRICITONS ON CERTAIN DISCLOUSRES AND SALES OF HEALTH INFORMATION; ACCOUNTING OF CERTAIN PROTECTED HEALTH INFORMATION DISCLOSURES; ACCESS TO CERTAIN INFORMATION IN ELECTRONIC FORMAT	
REQUESTED RESTRICTIONS ON CERTAIN DISCLOSURES OF HEALTH INFORMATION - Individuals will have the right to request that a covered entity restrict the disclosure of their protected health information of the individual and the covered entity must comply with the requested restriction except if the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment); and the protected health information pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.	Detail Information

Recovery Act
Subtitle D - Privacy Review

Title / Section	Link to Detail
Subtitle D -- Privacy	
DISCLOSURES REQUIRED TO BE LIMITED TO THE LIMITED DATA SET OR THE MINIMUM NECESSARY.— A CE or BA must continue to only use the amount of data necessary to meet the purpose or need of a request. This may mean by use of a Limited Data Set.	Detail Information

Recovery Act
Subtitle D - Privacy Review

Title / Section	Link to Detail
Subtitle D -- Privacy	
ACCOUNTING OF CERTAIN PROTECTED HEALTH INFORMATION DISCLOSURES REQUIRED IF COVERED ENTITY USES ELECTRONIC HEALTH RECORD - When you use an EHR, you must be able to account for all disclosures regardless of treatment, payment or operations.	Detail Information
PROHIBITION ON SALE OF ELECTRONIC HEALTH RECORDS OR PROTECTED HEALTH INFORMATION OBTAINED FROM ELECTRONIC HEALTH RECORDS.— a covered entity or business associate shall not receive remuneration in exchange for any protected health information of an individual unless the covered entity obtains an individual authorization.	Detail Information

Recovery Act
Subtitle D - Privacy Review

Title / Section	Link to Detail
Subtitle D -- Privacy	
ACCESS TO CERTAIN INFORMATION IN ELECTRONIC FORMAT - in the case that a covered entity uses or maintains an electronic health record an individual shall have the right to obtain a copy of information in an electronic format. The individual may direct the transmital of information directly to an entity or person designated by the individual.	Detail Information
Sec. 13406 CONDITIONS ON CERTAIN CONTRACTS AS PART OF HEALTH CARE OPERATIONS	
MARKETING - A communication by a covered entity or business associate that is about a product or service and that encourages the purchase or use the product or service shall no longer be considered health care operations. The CE or BA must obtain a valid authorization from the recipient for the communication or it must describe a drug or biologic that is currently prescribed for the recipient of the communication.	Detail Information

Recovery Act
Subtitle D - Privacy Review

Title / Section	Link to Detail
Subtitle D -- Privacy	
Sec. 13407 TEMPORARY BREACH NOTIFICATION REQUIREMENT FOR VENDORS OF PERSONAL HEALTH RECRODS AND OTHER NON-COVERED ENTITIES	
Sec. 13408 BUSINESS ASSOCIATE CONTRACTS REQUIRED FOR CERTAIN ENTITIES	
The regulations help define further what additional types of organizations would be considered a Business Associate, such as a Health Information Exchange Organization, Regional Health Information Organization, E-prescribing Gateway, or each vendor that contracts with a covered entity to allow that covered entity to offer a personal health record to patients as part of its electronic health record.	Detail Information
Sec. 13409 CLARIFICATION OF APPLICATION OF WRONGFUL DISCLOSURES; CRIMINAL PENALTIES	
A "person" who is subject to HIPAA criminal penalties now includes an employee or other individual; previously it was written that only a CE could be ciminally punished for a HIPAA violation.	Detail Information

Recovery Act
Subtitle D - Privacy Review

Title / Section	Link to Detail
Subtitle D -- Privacy	
Sec. 13410 IMPROVED ENFORCEMENT	
The act of investigating and imposing penalties for Privacy and Security violations will be improved.	Detail Information
An individual who is harmed by an act sharing their PHI may receive a percentage of any civil monetary penalty or monetary settlement collected with respect to such offense.	Detail Information
If it is believed that the interest of one or more of the residents of a State has been or is threatened or adversely affected by any person who violates a provision of Privacy regulations, the attorney general of the State, as parens patriae, may bring a civil action on behalf of such residents.	Detail Information
The Office of Civil Rights of the Department of Health and Human Services may continue the use of a corrective action plan without a penalty in cases where the person did not know (and by exercising reasonable diligence would not have known) of the violation involved.	Detail Information

Title / Section	Link to Detail
Subtitle D -- Privacy	
PART II -- RELATIONSHIP TO OTHER LAWS; REGULARTORY REFERENCES; EFFECITVE DATE; REPORTS	
Sec. 13421 RELATIONSHIP TO OTHER LAWS	
(a) APPLICATION OF HIPAA STATE PREEMPTION.—Section 1178 of the Social Security Act (42 U.S.C. 1320d–7) shall apply to a provision or requirement under this subtitle in the same manner that such section applies to a provision or requirement under part C of title XI of such Act or a standard or implementation specification adopted or established under sections 1172 through 1174 of such Act.	Detail Information

Recovery Act
Subtitle D - Privacy Review
Summary

Plain Language / Impacts

IMPACT: Previous incident and business associate language will need to be revised to reflect new definition.

IMPACT: All policies and procedures related to security and privacy will need to be reviewed/revised and/or cross referenced to reflect the use of EHR and this definition.

IMPACT: All policies and procedures related to security and privacy will need to be reviewed/revised and/or cross referenced to reflect the use of PHR and this definition. (As applicable to business use)

New Definition (although similar to that used in other healthcare regulations)

Recovery Act
Subtitle D - Privacy Review
Summary

Plain Language / Impacts

New Definition

IMPACT: 1) Education for CEs and BAs; 2) CEs Update Policies and Procedures; 3) CEs Update Risk Assessment; 4) CEs update BA Agreements; 5) BAs need to perform risk analysis and adopt full policies and procedures for Admin, Physical and Technical Safeguards.

There is no due date for the initial guidance for section 13401.

IMPACT: 1) BAs need to conduct risk analysis; 2) Create and/or revise admin, physical and technical safeguards policies and procedures; 3) Train staff who handle PHI on i) how to use PHI according to policies and procedures; ii) how/who to report a breach; and iii) other specific requirements as defined by the policies and procedures.

Plain Language / Impacts

IMPACT: 1) CEs and BAs need new policies, procedures, and training for breach reporting and notification, taking into consideration sub-sections (a) - (h); 2) CEs and BAs need to develop forms or mechanisms for breach notification, taking into consideration sub-sections (a) - (h).

First Guidance on specifying the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals due to the industry by the middle of April 2009.

Plain Language / Impacts

IMPACT: With or without the guidance CEs and BAs will need to decide on a methodology to secure PHI; and then to secure the PHI.

Guidance on how to make PHI unreadable or indeciperable is due to the industry by the middle of April 2009.

IMPACT: Both CE and BA must have policies, procedures, forms and training in place to deal with the federal breach law by September 2009.

Interim Final Regulations on IIHI breaches are due to be published in the federal register by the middle of August 2009; the provisions of this section, 13402, will apply to breaches discovered on or after 30 days after publication of the interim final regulations, by mid-September 2009.

Recovery Act
Subtitle D - Privacy Review
Summary

Plain Language / Impacts

IMPACT: within 6 months there will be some one in each region to ask questions about the privacy sections of ARRP 09.

IMPACT: 1) Education for CEs and BAs; 2) CEs and BAs update Policies and Procedures; 3) Update BA Agreements. The BA is now as responsible for privacy and security breaches and mistakes as is a CE.

Plain Language / Impacts

IMPACT: 1) BAs need to conduct risk analysis; 2) Create and/or revise administrative, physical and technical safeguards policies and procedures; 3) Train staff who handle PHI on, i) how to use PHI according to policies and procedures; ii) how/who to report a breach and iii) other specific requirements as defined by the policies and procedures.

IMPACT: 1) CEs will need to review/update policies and procedures for the individual right of request for restriction; and 2) CEs will need to train their staff on new/updated policies and procedures

The Guidance on minimum necessary is due by the middle of August 2010

Recovery Act
Subtitle D - Privacy Review
Summary

Plain Language / Impacts

IMPACT: 1) this is the use of a part of the HIPAA Privacy requirements in an area not intended under HIPAA Privacy; 2) this moves the mandate regarding the use of a limited data set (for research, public health activities and healthcare operations) into the regular work areas in a doctors office or hospital setting; 3) a limited data set has many data elements removed, including all demographics; 4) CEs will need to review/update policies and procedures, and provide new workforce training.
This area seems to be an acknowledgement that a minimum necessary decision is a subjective decision, and the industry would like a bit more structure in this area, so the requirement is to use the limited data set when possible.

The Guidance on minimum necessary is due by the middle of August 2010

Plain Language / Impacts

IMPACT:Previous to the ARRA Accouting for Disclosures excepted those disclosures for treatment, payment and healthcare operations. Now: 1) When a CE uses and electronic health record it will need a new policy and procedure for the HIPAA Privacy individual right of accounting, and train its workforce in this new area; 2) this area is complicated if the CE still has paper records (hybrid record where both paper and electronic elements are kept), as it will be much more difficult to give a TPO accounting of paper records a CE may have two different policies and procedures while they continue to maintain paper records

Regulations on what information shall be collected about each disclosure not later than 6 months after the date on which the Secretary adopts standards on accounting for disclosure described in the section 3002(b)(2)(B)(iv) [EHRs and accounting of disclosures] ; this is part of the new HIT Policy Committee that accepts standards, so there is no real date able to be suggested at this time.

IMPACT: 1) CEs and BAs will need to review/update sale of ePHI polieies and procedures; and 2) train their workforce of new/updated sale of ePHI policies and procedrues; 3) the policies, procdures and training must include the exeptions outlined below

Regulations on the sale of data from EHRs will be published by the middle of August 2010. The effective date will be 6 months after the publication of final regulations

Plain Language / Impacts

IMPACT: This is another area where access will be to both paper and electronic medical records 1) CEs will need to review/update polices and procedures dedicated to an individual's right of access to include data kept in electronic format; 2) CEs will have to train their workforce on the new/updated access policies and procedures

This section is a new definition of MARKETING; it states that the exceptions under the HIPAA Privacy marketing definition a part of HIPAA Privacy health care operations; 1) a health-related product or service that is provided by, or included in a plan of benefits; 2) for individual treatment; 3) for case management or care coordination of an individual, or to direct or recommend alternatives; UNLESS B) a CE receives or has received direct or indirect payment in exchange for making the communications; PLUS C) ARRA 09 EXCEPTIONS; 1) the communication describes a drug or biologic that is currently being prescribed, and; 2) the payment is a 'reasonable' amount, where; 3) CE obtains a valid HIPAA authorization in place; or 4) the communication is made by BA on behalf of CE, and consistent with BAA.

The effective date for this section shall be the middle of February 2010.

Recovery Act
Subtitle D - Privacy Review
Summary

Plain Language / Impacts
THE AREA OF PHRs is not outlined in this version **The Federal Trade Commission shall write Interim Final Regulations for breaches from vendors of PHRs by the middle of August 2010.**
IMPACT: Covered entities now have additional organizations being defined as Business Associates and they will be required to execute some type of contract provision covering the Privacy of PHI. If the covered entity is offering a Personal Health Record to the employee population, this entity should also be considered a Business Associate.
IMPACT: A CE will need to update a number of different policies and procedures now that individuals are subject to criminal penalties; and retrain its workforce.

Recovery Act
Subtitle D - Privacy Review
Summary

Plain Language / Impacts
Additional information is provided for improved enforcement in the detail tab.
IMPACT:1) all CEs will need to plan for formal investigations when a HIPAA compliant is filed against them; and 2) Since a person is now an individual if they commit willful neglect they will be investigated indivdually, and not just as an employee.
IMPACT: This is an additonal remedy for imporper use and disclosure of individuals' confidential medical information.
IMPACT: There will be interlocking/overlapping enforcement under HIPAA and ARRA 09; there may be numerous ripple affects through the HIPAA enforcement regulatory provisions; in other words the HIPAA regulatons will need to be read with the new regulations under the ARRA 09 privacy subtitle D.

Recovery Act
Subtitle D - Privacy Review
Summary

Plain Language / Impacts
IMPACT: Initial interpretation of the co-chairs is that pre-emption determination or rational will have to be reviewed against the new regulations, but the general spirit of the original language found in HIPAA stays intact.